Book Review: The Closing of the Net by Monica Horten

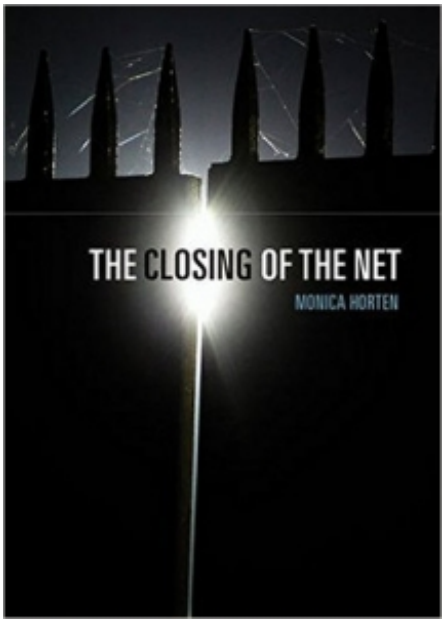
blogs.lse.ac.uk/lsereviewofbooks/2016/08/11/book-review-the-closing-of-the-net-by-monica-horten/

8/11/2016

In **The Closing of the Net***,* **Monica Horten** *confronts the issue of how corporate structural power has shaped the online world, transforming the ideal of the open internet into an increasingly closed, market-driven space with negative consequences for individual freedoms.* **Courteney J. O'Connor** *recommends this well-researched book as an extremely relevant addition to cyber-related literature that will also be of use to those working in the fields of politics, law and media.*

***The Closing of the Net*. Monica Horten. Polity. 2016.**

Find this book: amazon



Monica Horten's *The Closing of the Net* is a factually dense but eminently readable introduction to the issue of corporate structural power over the modern internet. Focusing on the way that political issues and events affect how the internet works for the individual, *The Closing of the Net* pairs the identification of key events with an on-the-ball and easy to understand analysis of their run-on effects. It is also made clear throughout the volume that far from dictating the policies by which telecommunications (telecoms) providers must abide, governments are regularly being influenced by these and other corporate entities.

In Chapter One, Horten begins with a discussion of the internet as both a source and tool of power for various parties (1-21). As a source of knowledge, the internet is a resource beyond compare. However, the telecoms providers that control both the physical infrastructure on which the Internet rests and our access to the internet itself have the power to control the extent of that access, including precisely what content the average user can find. Horten calls this the open internet vs. industrial control dichotomy, whereby commercial interests are negatively affecting the open internet empowerment narrative of earlier days (4).

Knowledge is identified early in the text as the primary function of the internet. Its 'knowledge function' in the cyber age is inextricably linked with the so-called 'security function' of the net, because the data stored on and transmitted through the internet can and is utilised for surveillance and security purposes (6). The book openly identifies the links between commercial control over vast data streams and the utility of that data, not only for state surveillance and security, but also for commercial behavioural analysis and content personalisation. Horten concludes that net neutrality – or an internet wherein all data is transmitted without discrimination or prioritisation – is being negatively affected, and is becoming an increasingly unlikely outcome given the majority control that telecoms providers have over internet infrastructure.

Image Credit: System Lock (Yuri Samoilov CC2.0)

Having identified data as 'the new ''oil" of the global economy' and a source of both knowledge and power (14), *The Closing of the Net* goes on to consider the legalities surrounding technologies such as cookie tracking and content filtering (because, yes, information exclusion can and does happen). Subsequent sections detail and analyse the influence of telecoms providers over both national and international law and policy pertinent to the collection, storage and sharing of data as well as cooperation with law enforcement. Given the relative novelty of cyberspace, comparative to the body of law regulating the domains of air, land, sea and outer space, cyber law has not kept pace with the development of the domain itself.

Communications providers are crucial to surveillance capabilities in the internet age: they are the entities that collect (the majority of) communications data. However, and depending on the provider in question, there is a limited timeframe within which law enforcement representatives can request an individual's communications data before providers are legally obliged to either delete or anonymise that data, rendering it far less useful. Horten avers that telecoms providers, particularly in the United States, are thus rightfully concerned about the liability risk of cooperation and the surrendering of data. This is one of the driving forces identified in the book behind the lobby groups representing the telecoms providers, who seek to sway or amend the drafting of policies and/or laws, either by subtly or overtly exercising the structural power of these providers. Horten makes the logical point that at this stage, the structural power of the telecommunications providers is both self-perpetuating and self-sustaining, limiting both the opportunity to make positive movement towards net neutrality and the efficacy of doing so (81). Given current political and security realities, individual privacy in cyberspace is quite correctly identified as an increasingly threatened notion.

Telecoms providers are not the only corporate bodies resistant to the idea of net neutrality. The entertainment industry also has an interest in restricting the storage and transmission of certain types of data, such as copyrighted material. Several cases of interest are identified in the book, not least of which is the ongoing legal case against Megaupload owner Kim Dotcom (128-36). By necessity, the entertainment industry in general is a proponent of content filtering and blocking as part of the effort to reduce revenue loss and intellectual property theft through content piracy. However, content filtering and blocking remain a legal uncertainty with some associated risk to the telecoms providers, and Horten argues (quite sensibly) that blocking can inadvertently affect sharing or storage of legal content (such as those with photos and personal documents stored on Megaupload) and/or the function of

unrelated IP addresses as a consequence of the original blocking target (88-125). This engages negatively with the right to freedom of expression, and contributes to the gradual decrease of internet freedom – or the closing of the internet.

The Closing of the Net is a well-researched and factually dense text. Despite the abundance of information, or perhaps supported by it, the book remains an easy read and neatly avoids the trap of being too dry to hold the interest of one who doesn't specialise in a cyber-related field. Considering the scope and breadth of the research and the clarity of the corresponding analysis, this book would be extremely helpful to those working in the fields of politics, law, media and technology as well as being a general interest text. It is an extremely relevant and timely addition to the growing body of cyber-related literature that I do not hesitate to recommend.

Courteney J. O'Connor is a PhD candidate with the National Security College of The Australian National University. Her research considers the securitisation of cyberspace and the development of cyber counterintelligence policy and practice.

Note: This review gives the views of the author, and not the position of the LSE Review of Books blog, or of the London School of Economics.